DETAILED ACTION

1. Claims 1-15, 19, and 20 are pending in this office action, claims 16-18 are canceled.

2. Applicant's arguments, filed January 23, 2008, are moot in view of the new ground of rejection.

Claim Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-15, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Berson et al. (U.S. Patent No. 6,123,456) in view of Eichert et al. (U.S. Patent No. 6,393,474).

Regarding claim 1, Berson et al. teaches a method of securing a network **interface** device installed on a host comprising:

- Initializing the network device without transmit functions (fig. 3, ref. num 306);
- Receiving notification that the host has been authenticated (fig. 3, ref. num 314); and

- In response to receiving notification that the host has been authenticated, enabling transmit functions of the network device (fig. 3, ref. num 318).

Berson et al. does not teach the network **interface** device is secured, but rather a network device attached to the host device is secured.

Eichert et al. teaches securing the network **interface** device without transmit functions (col. 7, lines 31-43) and the notification of authentication is received on the host **on which the network interface is installed** (col. 7, lines 31-43, the policy information is transferred to the smart NIC of the host that the NIC is installed).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine securing the network interface card from transmit functions, as taught by Eichert et al., with the method of Berson et al. It would have been obvious for such modifications because this securing can be used to control bandwidth congestion issues on a network with the use of a policy (see col. 7, lines 31-43 of Eichert et al.).

Regarding claim 2, Berson et al. as modified by Eichert et al. teaches wherein initializing the network **interface** device comprises initializing the network **interface** device without receive functions (see col. 4, lines 60-62 of Berson et al.).

Regarding claim 3, Berson et al. as modified by Eichert et al. teaches further comprising in response to receiving notification that the host has been authenticated, enabling receive functions of the network **interface** device (see fig. 3, ref. num 318 of Berson et al.).

Regarding claims 4 and 20, Berson et al. as modified by Eichert et al. teaches wherein enabling receive functions of the network **interface** device comprises routing received data to a network stack (see col. 2, lines 22-24 of Berson et al.).

Regarding claim 5, Berson et al. as modified by Eichert et al. teaches further comprising accessing a firewall policy server to download firewall policy information that is used by a firewall on the network **interface** device after enabling transmit functions of the network **interface** device (see fig. 3, ref. num 308 and 310 of Berson et al.).

Regarding claim 6, Berson et al. as modified by Eichert et al. teaches wherein accessing a firewall policy server is performed before transmitting or receiving data from other clients or servers (see fig. 3, ref. num 308 and 310 of Berson et al.).

Regarding claim 7, Berson et al. as modified by Eichert et al. teaches wherein accessing a firewall policy server comprises authenticating the firewall policy server (see col. 1, lines 43-45 of Berson et al.).

Regarding claim 8, Berson et al. as modified by Eichert et al. teaches wherein receiving notification that a host has been authenticated includes receiving notification that the host has been authenticated for a role, and wherein accessing a firewall policy server comprises downloading firewall policy information for the role (see col. 4, lines 60-62 of Berson et al.).

Regarding claim 9, Berson et al. as modified by Eichert et al. teaches further comprising receiving firewall policy information communicated to the host and using the firewall policy information at a hardware based firewall on the network **interface** device (see fig. 1, ref. num 112 of Berson et al.).

Regarding claim 10, Berson et al. teaches a network **interface** device for use in a host on a network, the network **interface** device comprising:

- A network port adapted to send and receive network information (fig. 2, ref. num 234); and
- A module that disables at least one of transmit and receive functionality to the network port of the network device until the network device is notified that the host has been authenticated (fig. 3, ref. num 314 and 318).

Berson et al. does not teach the network **interface** device is secured, but rather a network device attached to the host device is secured.

Eichert et al. teaches securing the network **interface** device without transmit functions (col. 7, lines 31-43) and the notification of authentication is received on the host **on which the network interface is installed** (col. 7, lines 31-43, the policy information is transferred to the smart NIC of the host that the NIC is installed).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine securing the network interface card from transmit functions, as taught by Eichert et al., with the device of Berson et al. It would have been obvious for such modifications because this securing can be used to control bandwidth congestion issues on a network with the use of a policy (see col. 7, lines 31-43 of Eichert et al.).

Regarding claim 11, Berson et al. as modified by Eichert et al. teaches further comprising a firewall that is adapted to prevent the network **interface** device from communicating with other devices according to firewall policy information stored at the firewall (see fig. 1, ref. num 112 of Berson et al.).

Regarding claim 12, Berson et al. as modified by Eichert et al. teaches further comprising nonvolatile memory, and wherein the firewall policy information is stored in the nonvolatile memory (see fig. 2, ref. num 216 of Berson et al.).

Regarding claim 13, Berson et al. as modified by Eichert et al. teaches wherein the network **interface** device is adapted to receive firewall policy information from a firewall policy server (see fig. 5 of Berson et al.).

Regarding claim 14, Berson et al. as modified by Eichert et al. teaches wherein the network **interface** device is embodied as a network interface card (see fig. 2, ref. num 250 of Eichert et al.).

Regarding claim 15, Berson et al. as modified by Eichert et al. teaches wherein the network **interface** device is embodied as a Secure CardBus network card (see fig. 2, ref. num 250 of Eichert et al.).

Regarding claim 19, Berson et al. teaches a method of securing a network **interface** device installed on a host comprising:

- Initializing the network device without receive functions (fig. 3, ref. num 306);
- Receiving notification that the host has been authenticated (fig. 3, ref. num 314); and
- In response to receiving notification that the host has been authenticated, enabling receiving functions of the network device (fig. 3, ref. num 318).

Berson et al. does not teach the network **interface** device is secured, but rather a network device attached to the host device is secured.

Eichert et al. teaches securing the network **interface** device without transmit functions (col. 7, lines 31-43) and the notification of authentication is received on the host **on which the network interface is installed** (col. 7, lines 31-43, the policy information is transferred to the smart NIC of the host that the NIC is installed).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine securing the network interface card from transmit functions, as taught by Eichert et al., with the method of Berson et al. It would have been obvious for such modifications because this securing can be used to control bandwidth congestion issues on a network with the use of a policy (see col. 7, lines 31-43 of Eichert et al.).

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRANDON S. HOFFMAN whose telephone number is (571)272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon S Hoffman/
Examiner, Art Unit 2136

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136